

Muhammad Ahmad Bashir (Curriculum Vitae)

Postdoctoral Research Fellow

International Computer Science Institute (ICSI)
1947 Center Street, Ste. 600, Berkeley, CA 94704

Email: mahmad@icsi.berkeley.edu
WWW: <https://ahmadbashir.com>

Research Interests

Security and privacy on web/mobile; internet measurement; limiting fraud and abuse

Education

- 2014-2019 **Doctor of Philosophy** in Computer Science - *Northeastern University*
 Thesis: *On the Privacy Implications of Real Time Bidding* advised by Christo Wilson
- 2008-2012 **Bachelor of Science** in Computer Science - *LUMS, School of Science and Engineering*

Employment History

- Oct 2019 - Present International Computer Science Institute (**Postdoctoral Research Fellow**)
- Jun 2018 - Aug 2018 International Computer Science Institute (**Research Intern**)
- June 2017 - Sep 2017 Facebook Inc. (**Threat Infrastructure, Security Engineering Intern**)
- May 2016 - Aug 2016 Facebook Inc. (**Online Safety, Security Engineering Intern**)
- Oct 2012 - Jan 2013 Max Planck Institute for Software Systems, Germany (**Research Intern**)

Honors and Awards

- 2018 Best Student Paper Award (**FPF Privacy Papers for Policymakers**)
- 2015 Best Paper Award (**Conference on Online Social Networks**)
- 2015 Best Paper Award (**Conference on Security and Cryptography**)
- 2012 Research Intern Fellowship (**Max Planck Institute for Software Systems**)
- 2011 Winner (**Ericsson – PTA Mobile Excellence Award**)
- 2011 Winner (**FPF Privacy Papers for Policymakers**)

Teaching Experience

- Fall 2018 Teaching Assistant / Guest Lecturer (**CS3700- Networks and Distributed Systems**)
- Spring 2018 Teaching Assistant / Guest Lecturer (**CS2550- Foundations of Cybersecurity**)
- Spring 2013 Teaching Assistant (**CS585: Service Oriented Computing**)
- Fall 2012 Teaching Assistant (**CS582: Distributed Systems**)
- Spring 2012 Teaching Assistant (**CS380: Databases**)

Selected Publications

IMC '19	A Longitudinal Analysis of the ads.txt Standard <ul style="list-style-type: none">• A 15-month long study analyzing the adoption of the ads . txt standard by Alexa-100K websites.
NDSS '19	Quantity vs. Quality: Evaluating User Interest Profiles Using Ad Preference Managers <ul style="list-style-type: none">• First large-scale study of the “interests” inferred by ad networks using Ad Preference Managers.• We investigate how these interests were inferred and how useful they were according to the users.
IMC '18	How Tracking Companies Circumvented Ad Blockers Using WebSockets <ul style="list-style-type: none">• First large-scale study of the “interests” inferred by ad networks using Ad Preference Managers.• We investigate how these interests were inferred and how useful they were according to the users.
PETS '18	Diffusion of User Tracking Data in the Online Advertising Ecosystem <ul style="list-style-type: none">• We model how user tracking data propagates in the advertising ecosystem because of RTB.• We model the efficacy of ad and tracker blocking extensions at protecting users' privacy.
IMC '16	Recommended For You: A First Look at Content Recommendation Networks <ul style="list-style-type: none">• First look at how content (ads and recommendations) is served by CRNs.• Highlights the inconsistencies in how the content is served and calls for stronger regulations.
USENIX '16	Tracing Information Flows Between Ad Exchanges Using Retargeted Ads <ul style="list-style-type: none">• Proposes a generic methodology to detect information sharing between ad networks.• Detects 31% of cookie matching partners which were missed by prior methods.
COSN '15	Strength in Numbers: Robust Tamper Detection in Crowd Computations <ul style="list-style-type: none">• Detection of large-scale (Sybil-tampered) crowd computations in Online Social Networks.• Dataset consists of roughly 300M Twitter users and 30K businesses with 341K reviews from Yelp.
USENIX '14	Towards Detecting Anomalous User Behavior in Online Social Networks <ul style="list-style-type: none">• Detection of anomalous identities, using PCA, on Facebook used in diverse attack strategies.• Includes a case study on Facebook Ads to detect anomalous clicks.

Ongoing Work

1. Cross Device Tracking

- A comprehensive study of the state of cross-device tracking and the underlying mechanisms used.

2. SDKs & Android Permissions

- A methodological way of examining which SDK requested which Android permission.

3. Consent Management Platforms

- A study on consent management platforms in EU-based websites.

Technical Skills

- **Programming Languages:** Python, Javascript, Java, Hack, C++, SQL
- **Web Development:** HTML5, Nodejs, Express, Django
- **Miscellaneous:** Spark, Selenium